

REMARKS

Claims 1 to 12 are pending in the application.

Rejection under 35 U.S.C. 103

Claims 1-12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Russell et al.* (US 6,568,595).

According to the examiner, *Russell* teaches a method of selling services and/or products by using telecommunications link, wherein the user selects a provider's product, transmits an identification code (as set forth in claim 1), the provider sends codes to the code verification system (claim 1: symbol reader), the system triggers a non-contact code verification which would compare the codes to find the proper one and grants access to the user upon code verification.

Examiner points out that even though *Russell* does not specifically mention the mobile communication network it is however well-known in the art to use wireless communication to access the Internet. Examiner also states that it would have been obvious to have the communication device (phone or computer connected through cellular network) to save the data to ensure a record is saved in case of disputes.

In Response to Arguments the examiner points out that as regards "non-contact" verification the prior art teaches ensuring the code is proper and therefore it would have to compare it or else it would not know whether the code is correct.

Applicant has amended claim 1 to further clarify the steps involved. Step b) now makes clear that the identification code, which identification code is user-specific and saved in a mobile telecommunication unit of the user, is directly transmitted by the mobile telecommunication unit of the user through the supraregional communications link to the offeror.

Applicant has further amended claim 1 to better define the step d) of non-contact identification verification in that, when the user enters with the mobile telecommunication unit a predetermined physical range of the identification verification system, the saved identification code is directly retrieved by the identification verification system from the mobile telecommunication unit of the user through a local area communications link.

Russell discloses a method for enabling electronic commerce. The method involves a Java-Applet that enables electronic commerce and is embedded within an HTML-encoded document stored in an HTTP server at a predetermined URL. To activate the electronic commerce capability at a Java-enabled Internet terminal, a code symbol such as a magnetic strip or bar code encoded with the URL must be read by a code symbol reader provided at the Internet terminal. This causes the corresponding HTTP document to be automatically accessed and displayed at the terminal. The electronic-commerce enabling Java-Applet is then initiated so that the customer can now conduct an electronic-commerce transaction over the Internet, i.e., the disclosure of *Russell* concerns the steps **before the actual commerce transaction can take place.**

In contrast to this, the method of instant claim 1 concerns the actual transaction that is being performed by telecommunication. The method of claim 1 requires that the user selects an offer and transmits an identification code to the offeror, which identification code is user-specific and saved in a mobile telecommunication unit of the user and transmitted directly by the mobile telecommunication unit of the user through the supraregional communications link to the offeror.

Russell does not disclose such a step of directly transmitting the user-specific identification code, stored in a mobile telecommunication unit of the user, by means of the mobile telecommunication unit through the supraregional communications link to the offeror. *Russell* discloses in col. 19, line 60, to col. 20, line 11, that (emphasis added):

“Optionally, other types of **information can be encoded within the transaction-enabling mag-stripe card** of the present invention so as **to carry out transaction-access authorization**, and other security functions known in the art (e.g., expiration date control, etc.). For example, expiration-data control can be carried out by encoding certain bits along a particular data track of the mag-stripe to represent the expiration date of the transaction-enabling card. **Restricted-user control can be carried out by (1) encoding certain bits along a particular data track of the mag-stripe to encode a personal identification code for access** by the HTTP server hosting the transaction-enabling HTML document, **and (2) requiring the user to manually enter a preassigned access code** when the transaction

"home" Web page is displayed, thereby **completing the security protocol** established by the transaction service provider. Notably, such security techniques can be carried out using URL-encoded (1-D and 2-D) bar code symbols in a manner similar to that described hereinabove."

The examiner reduces in his arguments the step b) of instant claim 1 to "transmits an identification code", but instant claim 1 defines specific features in regard to the transmission of the identification code, namely:

- the identification code is user-specific and **saved in a mobile telecommunication unit** of the user
- the saved identification code is **directly transmitted by the mobile telecommunication unit through the supraregional communications link to the offeror**;

The identification code transfer is thus performed directly by the telecommunication unit (i.e. mobile phone) by means of telecommunication **through the supraregional communications** link.

The identification code according to *Russell* is encoded in a mag stripe of a card. A card with a magnetic stripe is not a telecommunication unit; it has no telecommunication functionality; it cannot transmit directly data through a supraregional communications link to the offeror. The card of *Russell* must be read out by a reader at a terminal. The terminal may provide telecommunication capabilities but not the magnetic stripe card where the identification code is saved. Such a magnetic card cannot suggest a mobile telecommunication unit that transmits directly the identification code through supraregional communications link to the offeror.

Russell discloses wireless communication 5 (col. 7, lines 3-7) between server 2 and client system 3 but the client system belongs to and is operated by the commerce system; the client system is not a user-owned system; the wireless communication disclosed is used within the commerce system and does not relate to communication between the customer and the commerce system. The customer or user must use a terminal (belonging to the commerce system) to have access to the Internet-based commerce system.

Examiner argues that it would be obvious to modify the system of *Russell* to have

wireless communication. However, the system of *Russell* is based on user verification through an identification code on a magnetic stripe card at the terminals (col. 20) - the terminals have specific readers to enable this function. There is no teaching or suggestion to eliminate a terminal with a card reader for magnetic stripe cards and the correlated magnetic stripe cards with their safety features since these terminals are the access points that enable the e-commerce functions of the commerce system and to provide instead a system that is based on a mobile telecommunication unit of the user where an identification code is saved that is to be transmitted to the offeror by telecommunication. Such a modification is not apparent and not obvious as it would eliminate the commerce system access points of the *Russell* system.

The examiner also reduces in his arguments the step d) of instant claim 1 to "the system triggers a con-contact code verification which would compare the codes to find the proper one" but instant claim 1 defines specific features in regard to the non-contact verification, namely:

- the non-contact identification verification begins when the user enters with the mobile telecommunication unit a predetermined physical range of the identification verification system;
- the saved identification code is directly retrieved by the identification verification system from the mobile telecommunication unit of the user through a local area communications link.

Thus, according to the present invention as claimed, the transmittal of the identification code (step b)) and the retrieval of the identification code (step d)) in accordance with the non-contact identification verification are carried out through direct telecommunication between the mobile telecommunication unit of the user and the offeror, respectively, the identification verification system. This is illustrated in the only Figure by the radio tower and mobile network M as regards step b) and by the arrows 4, 6 indicating the local network and local data transmission in regard to step d).

In *Russell* there is no disclosure as regards an identification code that is being saved in the mobile telecommunication unit of the user and that is directly retrieved by the identification verification system when the user with his mobile telecommunication unit enters a physical range of the identification verification system. All actions in *Russell* center

around the use of a terminal ("Internet Transaction-Enabling Terminal") as an access point to the commerce system. The telecommunication features reside exclusively within the commerce system and the associated terminals of various kinds hooked up through telecommunication lines to the Internet server of the commerce system. There is no mention of a mobile telecommunication unit of the user having stored therein the identification code; the access terminals disclosed in *Russell* are always system-owned terminals and never mobile telecommunications units of the user. There is never a telecommunication between a mobile telecommunication unit of the user and the commerce system or its terminals.

In *Russell*, the only type of verification based on a personal identification code relates to the magnetic stripe discussed above (col. 20, line 3) and there is no disclosure in regard to having a personal identification code on a mobile telecommunication unit of the user, wherein the mobile telecommunication unit, on the one hand, directly transmits the code to the offeror to initiate a transaction and, on the other hand, the code is retrieved directly from the mobile telecommunication unit by the identification verification system.

In regard to step c) applicant would like to stress again that the method of the present invention comprises the feature that the offeror assigns in its computer system the identification code to the offer selected by the user and makes a reservation for the offer with assigned identification code. The offeror transmits the reservation together with the assigned identification code to an identification verification system.

Such features are not disclosed in *Russell*. *Russell* only discloses an access system for Internet commerce. *Russell* teaches that upon code read-out and verification the HTTP document is displayed on the Internet terminal used by the user and the Java Applet is launched so that now through the Internet terminal e-commerce transactions are enabled, i.e., it is at this point of interaction that the user may select an offer.

The actual steps in regard to the commercial interaction between the user and the commerce system are never disclosed. The only reference to transactions to be performed through the Web browser can be found in col. 20, lines 50 to 59, of *Russell*. This disclosure merely provides a list of possibilities, such as financial transactions, account management, ticket purchase. Nothing is disclosed in regard to the individual steps that are required in order to carry out and complete such a transaction. Nothing is disclosed with respect to a

reservation being made by using the personal identification code and transfer of such a reservation to a verification system for later retrieval. There is not even described how a purchase transaction is to be performed and which steps are carried out.

Russell does not disclose or suggest that an personal identification code is assigned to an offer selected by the user and that the offeror assigns the identification code to the offer selected by the user and makes a reservation for the offer with the assigned identification code and, subsequently, the offeror transmits the reservation together with the assigned identification code to an identification verification system. Such steps are not obvious in view of the lack of any particular sin *Russell* regarding the transactions.

It is therefore respectfully submitted that the invention as now claimed is not obvious in view of *Russell*. Reconsideration and withdrawal of the rejection of the claims under 35 USC 103(a) are respectfully requested.

CONCLUSION

In view of the foregoing, it is submitted that this application is now in condition for allowance and such allowance is respectfully solicited.

Should the Examiner have any further objections or suggestions, the undersigned would appreciate a phone call or **e-mail** from the examiner to discuss appropriate amendments to place the application into condition for allowance.

Authorization is herewith given to charge any fees or any shortages in any fees required during prosecution of this application and not paid by other means to Patent and Trademark Office deposit account 50-1199.

Respectfully submitted on December 2, 2010,

/Gudrun E. Hockett/

Ms. Gudrun E. Hockett, Ph.D.
Patent Agent, Registration No. 35,747
Schubertstr. 15a
42289 Wuppertal, GERMANY
Telephone: +49-202-257-0371
US-Fax: (877) 470-9712
gudrun.draudt@t-online.de

GEH